di Raffaello De Masi

DataFellows F-Secure 4.0.1

'Sta storia dei virus comincia a non piacermi. Dopo tre puntate di ABC sull'argomento, e la prova di due pacchetti analoghi su questo numero, ho notato che la gente comincia a guardarmi in maniera strana. Quando sono passato l'ultima volta in redazione, nessuno mi ha voluto dare la mano, tutti più o meno educatamente si sono allontanati adducendo motivi di impegni già assunti, con la coda dell'occhio ho visto Andrea che strofinava la sedia su cui mi ero seduto con un panno imbevuto d'alcool; solo Rino, il più diplomatico, mi ha chiesto se mi sentissi proprio bene! Ohé, ragazzi, si tratta di virus informatici, non fatevi idee strane. Chissà cosa hanno pensato; fatto sta che ho capito l'antifona e, insalutato ospite, me ne sono andato, anche perché dovevo passarmi la pomata sulle croste verdi che da un po' di tempo mi sono uscite sul viso e sulle mani. Valli a capire, gli amici!

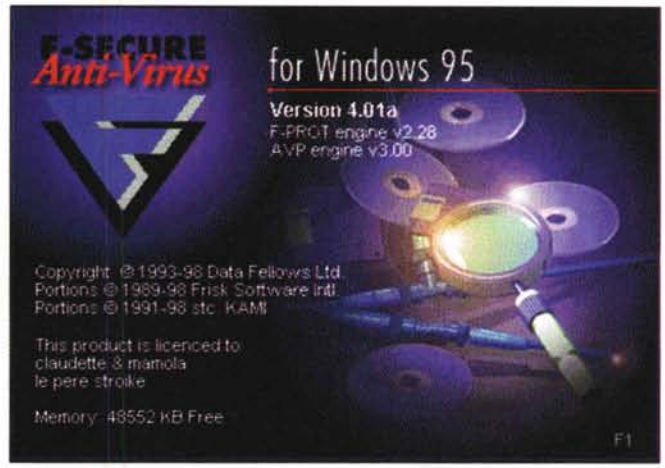
Fatto sta che ho notato che l'argomento virus, inaspettatamente, ha risvegliato un profondo interesse da parte dei lettori. Pochi, infatti, immaginavano che la loro produzione fosse, come dire, giornaliera, e che la loro presenza si aggirasse sulle diverse decine di migliaia di tipi diversi. E, nella casella di posta, l'argomento virus è divenuto, in questo periodo, prevalente. Manco a dirlo, molti mi hanno scritto preoccupati di strani sintomi avvertiti durante l'uso della loro macchina, di chiusure dei programmi del tutto inaspettate, di sistemi che si bloccano inaspettatamente (ricordo il banner della casella di posta di Leo Sorge: "Windows che s'inchioda non fa notizia, Windows che funziona, sì!") di collegamenti Internet improvvisamente abortiti. E' facile farsi prendere dalla psicosi, ma è il caso di ricordare che, ringraziando Dio, non è poi tanto facile infettarsi, specie se si usano certe precauzioni.

DataFellows F-Secure 4.0.1

Produttore :
DataFellows F-Secure, v. 4.0.1
Data Fellows Group
PL 24, FIN-02231
Espoo, Finland
http://www.DataFellows.com

Distribuito in Italia da:
Direzione Commerciale e Tecnica
Symbolic
Viale Mentana, 29
43100 Parma
http://www.symbolic.it

Prezzi: (iva esclusa)
Lit. 400.000



Lo splashscreen di F-Secure.

L'ambiente principale del programma, con il toolbar personalizzabile e le icone dei componenti e dei task.

Ed ecco quindi, accanto alla prova del classico tra i classici, il test di un bel pacchetto antinfluenzale proveniente da climi nordici, addirittura dalla Finlandia, dove, fosse solo per la latitudine, certo di malattie virali da raffreddamento ne sapranno qualcosa. Un pacchetto, come vedremo, agile, raffinato, efficiente, paragonabile con i mostri sacri del settore, e che in più ha un certo profumo di esoticità e originalità che non guasta.

F-Secure, per mettersi al sicuro

Perdonate l'ignobile gioco di parole, ma mi è venuto spontaneo. Fatto sta che questo pacchetto mi è parso subito interessante e, per così dire "simpatico", non foss'altro, come dicevamo, per differenziarsi dalla massa adepta alle pur sicure protezioni di MCAfee e NAV. Oltre, comunque, alle pure e semplici considerazioni circa l'originalità, F-Secure si fa notare per essere un ambiente di solida costruzione, ben articolato e caratterizzato da un potente background conoscitivo del problema. I risultati, in termini di efficacia e di copertura del problema possono essere riassunti tenendo conto della particolare attenzione prestata dagli implementatori alle seguenti caratteristiche:

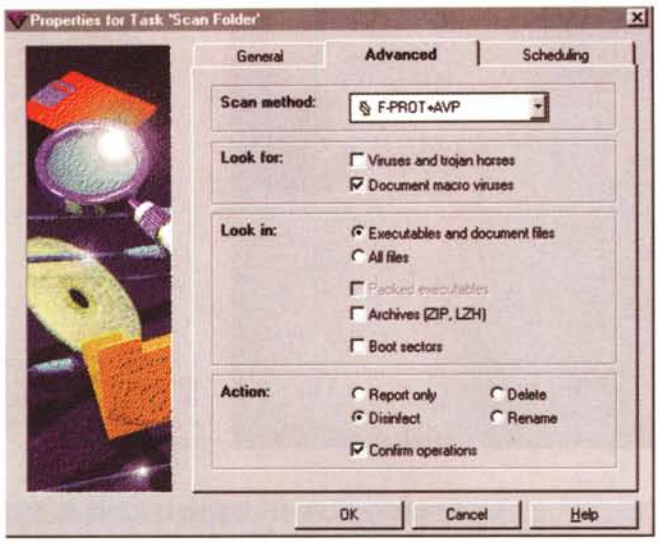
- amministrazione centralizzata della gestione della protezione e possibilità di intervenire in ogni momento sulle tecniche di manutenzione;
- trasparenza pressoché assoluta per l'utente finale;
- protezione in tempo reale garantita ai più alti livelli;
- ampio supporto di diversi sistemi operativi e piattaforme hardware;
- visione integrata della difesa dai virus come parte di un più ampio ambiente di protezione;
- supporto diretto illimitato delle esigenze degli utenti.

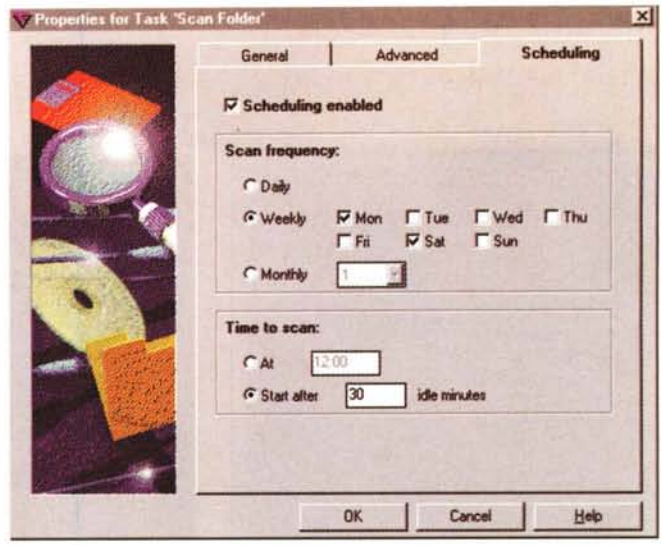
In altri termini, DataFellows considera il suo pacchetto non come un semplice prodotto software, ma come un servizio fornito all'utente. Ho potuto, in quest'ottica, sperimentare come risposte a quesiti vengano fornite a distanza di qualche ora o, al massimo, il giorno successivo. Ho avuto, in questo senso, il piacere di avere anche una fitta corrispondenza con Mikko Hernanni Hypponen (Mikko.Hipponen@DataFellows.com), persona di grande competenza e di estrema cortesia, cui, d'altro canto, è dovuta la messa a punto di parte del codice del pacchetto e cui sono da accreditare riconoscimento di numerosi virus e delle relative stringhe di individuazione.

A testimonianza della completa attenzione posta dalla DataFellows nei riguardi del problema, sarà sufficiente ricordare che F-Secure è disponibile per un'infinità di ambienti e di configurazioni diverse; nello stesso CD sono comprese versioni per Windows 3.1, W95 e 98, Windows NT, OS/2, DOS in tutte le versioni, PC-98 e DOS/V. Ma l'ambiente si estende a comprendere Server come Windows NT Server, Novell NetWare e OS2/Warp, e gateway come firewall CVP-compliant, Internet Mail, MS Mail, Microsoft Exchange, Lotus Notes, Lotus cc:Mail, Novell GroupWise e MHS Mail.

F-Secure anche in area Mac

DataFellow offre agli utenti Apple un pacchetto essenzialmente identico a quello descritto e dedicato all'ambiente Mac. Si tratta di un programma costruito sullo stesso motore e articolato nelle parti e con le procedure descritte, fatta ovviamente la debita distinzione tra le tipologie di virus e il diverso ambiente di utilizzo. La manualistica è anche qui fornita sotto forma .PDF, e, obbediente alla filosofia di utilizzo anche su macchine datate, l'applicazione gira anche su vecchi Mac dotati del 68040. L'aggiornamento delle librerie è continuo e paragonabile all'altro ambiente, e avviene con la stessa tecnica del Web Club. Notevole qui la velocità di scansione, anche se il caricamento del Gatekeeper rallenta un poco lo startup iniziale. Il prezzo è di poco superiore a quello indicato per la versione Windows.





Le finestre di gestione dell'attività del pacchetto; si noti come sia possibile selezionare difese contro cavalli di Troia e macrovirus, scansionare archivi e .EXE, schedulare forme diverse di scansione.

Base comune della linea di prodotti è una tecnologia, proprietaria di DataFellows, definita CounterSign, che combina diverse tecniche complementari di scansione; questa architettura di protezione definita multitiered (multistrato, multigradino) include scansione su base di verifica incrociata di "signature" (la ricerca e la verifica del tratto di codice sospetto viene eseguita in diverse prospettive), analisi euristica dell'ambiente sospetto e verifica del checksum, protezione a vari livelli dei dati e dei file. F-Secure è il primo prodotto a usare, in ogni momento, un approccio "a certificazione" delle macro su documenti o spreadsheet. La cosa è importante e significativa se si considera che, in un network, il modulo F-Secure Anti-Virus Macro Control può essere facilmente configurato dall'amministratore di rete per garantire macro autentiche e autorizzate nei confronti di altre che, non riconosciute come specifiche dell'ambiente di network, potrebbero indicare un possibile inquinamento. Analoga potente protezione è garantita nei confronti dei pericoli d'accesso attraverso firewall, cosa sempre possibile e sovente probabile quando ambienti si aprono verso l'esterno attraverso reti remote o attraverso Internet. In questo caso F-Secure Antivirus for Firewalls analizza e rimuove i virus prima dell'accesso al network, in questo integrandosi perfettamente con l'ambiente parallelo F-Secure Network Management. Infine F-Secure Antivirus mail Gateway supporta tutti i maggiori client di e-mail, come pure tutti i protocolli correnti incluso POP3, SMTP, UUPC via dial-up, ISDN e linee condivise. Come nella maggior parte degli prodotti del genere, l'efficienza e la garanzia offerta dal pacchetto è legata, più che sull'aggiornamento del codice, sulla tempestiva disponibilità delle informazioni di identificazione relative agli ultimi virus scoperti. Questo avviene, qui, attraverso l'iscrizione gratuita al DataFellows Web Club, che, attraverso connessioni via Internet permette di scaricare gli ultimi aggiornamenti e di accedere a un'ampia libreria tecnica dedicata soprattutto ad amministratori di rete e a ricercatori nel campo.

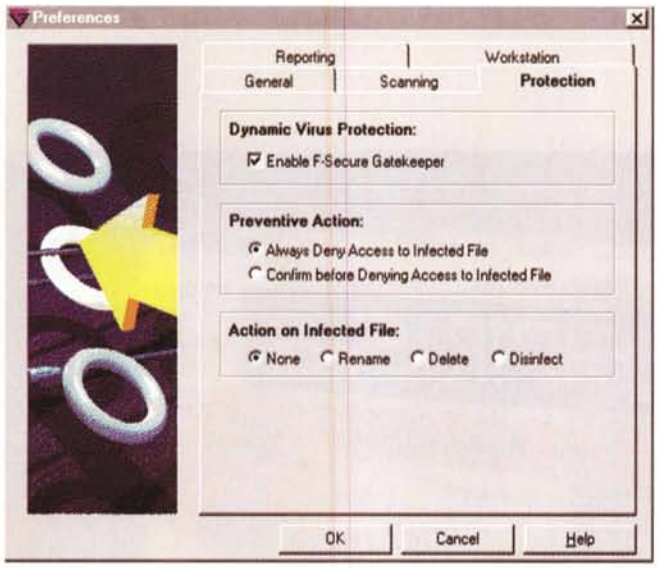
La cura riservata da DataFellows all'ambiente network è davvero apprezzabile; l'amministratore può installare versioni per così dire desktop sulle postazioni presenti nel network, inviare ai singoli utenti aggiornamenti successivi con un solo click del mouse, ricevere automaticamente report quando vengono incontrati virus, file probabilmente infetti, o solo comportamenti sospetti. E' possibile eseguire verifiche e scansioni su una stazione remota, cambiare, allo stesso modo, setting e configurazioni, gestire l'SNMP (Simple Network Management Protocol) per operazioni di alert automatici, gestire le installazioni e gli update attraverso l'SMS (il Systems Management Server di Microsoft).

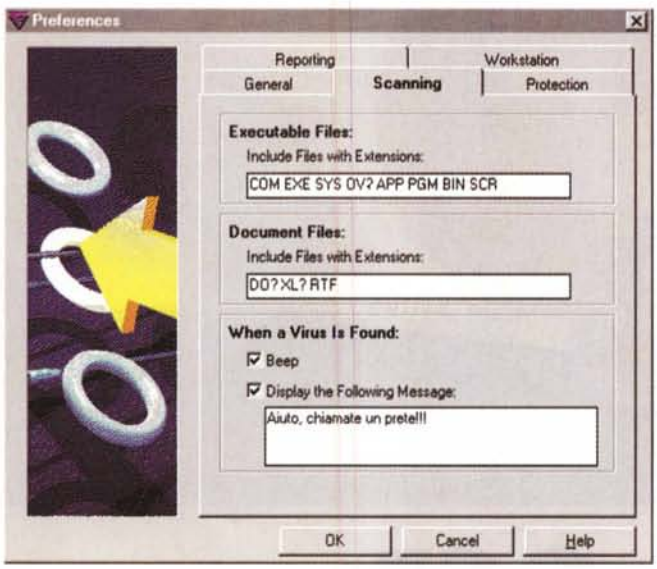
Anche l'ambiente end-user è molto ben realizzato e gradevole, ancorché concepito per essere, per quanto possibile, trasparente all'utente. Il toolbar del programma è completamente personalizzabile, il database dei virus è gradevolmente e curiosamente commentato, l'F-Secure Antivirus Service aggiorna automaticamente i database su network, anche in assenza dell'utente, il supporto multilingua permette di scegliere l'ambiente d'uso più facile. Tutto, insomma, è fatto in modo da impicciare il meno possibile, pur garantendo il massimo della protezione in ogni momento.

Come usare F-Secure

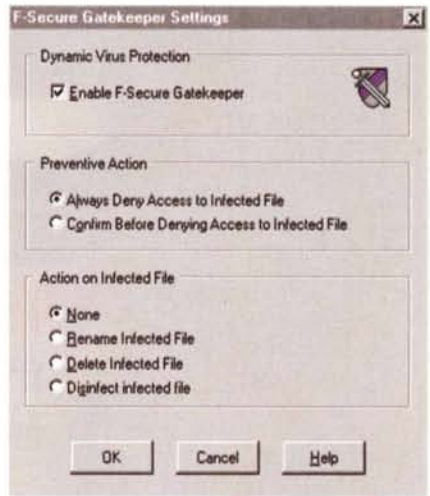
Installare F-Secure significa, come al solito, passare attraverso la ben nota procedura. Come dicevamo il CD contiene le versioni per molte piattaforme, oltre ai dimostrativi delle stesse e i manuali in diverse lingue nel solito formato .PDF (duro da leggere, il finlandese!). Appena lanciato il package chiede il numero di serie e si può sostenere che, da questo momento in poi, F-Secure non disturberà quasi più.

L'F-Secure Antivirus Web Club; l'aggiornamento alle librerie antivirus è gratuito.





F-Secure GateKeeper, l'ambiente di monitoraggio trasparente, abilitato allo startup, che verifica l'accesso a file provenienti dall'esterno (dischi, network, Internet).



In base al principio di lasciare l'utente libero di badare alle sue cose, principio questo comune a molti antivirus, F-Secure viene lanciato allo startup, sotto forma di F-Secure-Agent, un ambiente di monitoraggio che verifica e controlla continuamente attività sospette e azioni non consentite. A F-Secure comunque si può accedere in ogni momento lanciandolo dalla barra delle applicazioni e ci ritroveremo in un'amichevole finestra che non abbisogna certo di soverchie spiegazioni. In alto avremo una barra-palette dei comandi con diciassette icone che permettono di lanciare scansioni più o meno guidate, o di creare task, progetti-ambienti di scansione in cui saranno schedulati tempi, obiettivi, memorie di massa da sottoporre a controllo. Come al solito, anche qui sarà possibile filtrare le operazioni da eseguire (ad esempio se si sospetta la presenza di un macrovirus, sarà inutile analizzare gli .EXE o i .DLL, tanto per dire). Ovviamente sarà sempre possibile inserire nel controllo gli archivi e i settori di boot; se poi si è dei soliti smanettoni che preferiscono usare estensioni proprie, appare evidente che occorrerà avvertire F-Secure della cosa. Lo scheduling del controllo può avvenire a intervalli scelti dall'utente e quando si verificano certe situazioni di disponibilità della macchina.

I risultati dell'operazione possono essere serviti in vario modo, tra cui, disinfezione automatica o manuale, tempi di esecuzione del programma, tipologia delle eventuali infezioni e sorte dei file sottoposti a cura; in base a un'articolata tabella delle opzioni d'uso si possono salvare i report delle analisi, escludere tipi particolari da tutte le scansioni, editare un particolare avviso di attenzione, sviluppare tecniche preventive di difesa (come negare l'accesso a file infetti, e/o rinominare gli stessi), scegliere di terminare certe operazioni quando l'infezione avviene in ambiente DOS. Se usato in un network, F-Secure offre prestazioni e caratteristiche aggiuntive, come comunicazione automatica in caso di arrivo di aggiornamenti, invio automatico del report all'amministratore del sistema, gestione delle comunicazioni anche tra piattaforme diverse.

Un'intera sezione del manuale è dedicata agli amministratori di rete; la documentazione presente è molto ben fatta e curata (come curatissima è l'area di documentazione dei virus) e il System management, fatte le debite differenze, è ancora chiaro e amichevole, senza mai indulgere a complesse tecniche specialistiche. Vari ambienti, da UNIX a Microsoft LAN Manager, da VINES a Novell sono tutti supportati, e la gestione delle particolari caratteristiche, come diritti d'accesso, restrizioni, individuazione delle workstation, distribuzione delle installazioni e degli update, sono sempre facilmente accessibili attraverso la classica interfaccia a linguette (si possono anche distribuire task e report).

Conclusioni

F-Secure è un eccellente pacchetto antivirus, continuamente aggiornato e potentemente articolato a coprire esigenze diverse e ambienti anche molto diversificati tra loro. Questa è la sua arma più forte, assieme alla sua indubbia facilità d'uso e a una notevole rapidità nella sua azione di scansione e disinfezione.

Inevitabile il confronto con Norton AntiVirus, la cui prova appare su queste stesse pagine. NAV ha, sicuramente, dalla sua la possibilità di isolare in quarantena file sospetti fino alla definizione della loro sorte e/o alla risposta da parte di Symantec sulla natura dell'infezione. F-Secure possiede invece una documentazione tecnica invidiabile, sia sotto forma di manuale sia in linea con http://www.europe.datafellows.com, e una libreria dei virus interessante. I due prezzi, come vedete, non sono sovrapponibili, ma gli aggiornamenti di F-Secure sono a vita e lo stesso disco contiene diverse versioni per altrettanti ambienti.

In conclusione, scegliete quello che preferite, ma, soprattutto, difendetevi bene contro le influenze e gli attacchi virali. Fortunatamente, per quelli da virus informatici, gli antibiotici informatici funzionano alla perfezione.

MC